DEPARTAMENTO DE ELECTRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA

MESTRADO INTEGRADO EM ENG. DE COMPUTADORES E TELEMÁTICA
ANO 2015/2016

FUNDAMENTOS DE REDES

LABORATORY GUIDE NO. 2

Objectives

- The Virtual LAN (VLAN) concept
- Analysis of the IEEE802.1Q VLAN protocol
- Interconnection of VLANs
- The Spanning Tree routing concept
- Analysis of the IEEE802.1D Spanning Tree protocol.

Duration

- 4 weeks

1. Evaluation

- This guide will be evaluated by a written test composed by multiple choice questions.
- In order to prepare for the written test, students should make during all laboratory classes an own report with the conclusions taken on all experiments including the captures showing all results supporting them.

2. Additional documents necessary for this guide

- "Configuration Commands of CISCO Router".
- "D-Link Switch Manual".
- "D-Link CLI Reference Manual".

3. Mandatory actions at the end of each class

At the end of each class, the network equipment must be reset to its default configuration before switching them off.

☞ **Reset to default configuration of CISCO Router**

To reset the CISCO Routers to its default configuration, first, run the following command:

```
router#write erase
```

and, then, switch off the Router.

☞ **Reset to default configuration of D-Link Switch**

To reset the D-Link Switch to its default configuration, first, run the following command:

```
DES-3026:4#reset config
```

and, then, switch off the Switch.

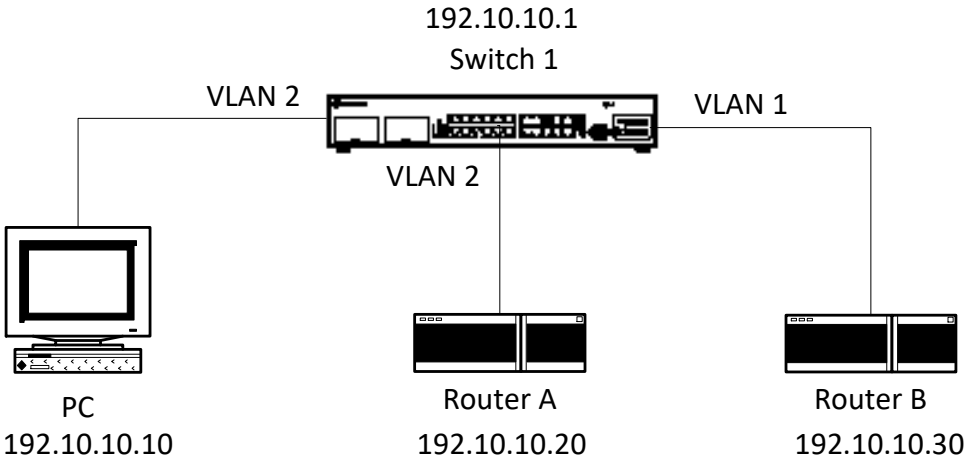
4. Experiments with Virtual LANs

1.1. Set up the network shown in the following figure and configure all IP addresses with netmask 255.255.255.0. In Switch 1, check that the Spanning Tree protocol is disabled and configure two VLANs in the following way[1]:

a) ports numbered 1 to 4 belonging to VLAN 1 (the default VLAN);

b) ports numbered 5 to 8 belonging to VLAN 2.

Connect the PC and Router A to VLAN 2 ports and Router B to a VLAN 1 port, as specified in the figure.



☞ **Configuration of STP in D-Link switches**

"D-Link CLI Reference Manual", pages 74-80

☞ **Configuration of VLANs in D-Link switches**

"D-Link CLI Reference Manual", pages 125-127

1.2. Using the RS-232 console access to the equipment, run the ping command to check which pairs of equipment (including Switch 1) have IP connectivity. Verify that only equipment in the same VLAN has IP connectivity.

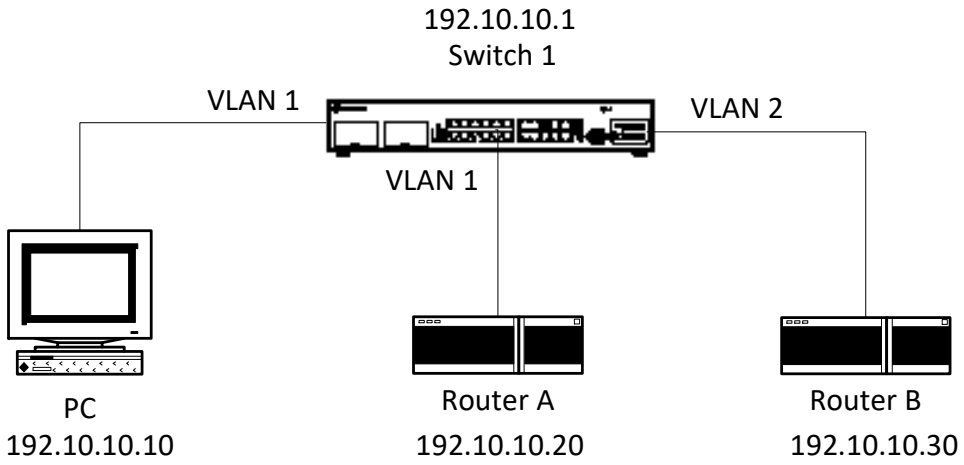
1.3. Using the RS-232 console access to the equipment, register and justify the MAC Address Table of Switch 1. In particular, check that the VLAN information is in accordance with the network setup.

1.4. Start a capture with the WireShark on the PC and set an appropriate filter to display ARP and ICMP packets. Using the RS-232 console access to the equipment, run the ping commands specified in the following table. For each run, register the connectivity and the filtered packets. Justify the results obtained on each case.

[1] The switches have a CPU running the switch management system. The CPU can be seen as an internal host, with a MAC address, connected to an internal switch port on the default VLAN which is VLAN 1.

Ping from:	Ping to:	Connectivity (yes or no)	Filtered packets
Router A	Switch 1		
Router A	Router B		
Router A	192.10.10.34		
Router B	Switch 1		
Router B	Router A		
Router B	192.10.10.34		
Switch 1	Router B		
Switch 1	192.10.10.34		

2.1. In Switch 1, change the cables in order to connect the PC and Router A to VLAN 1 ports and Router B to a VLAN 2 port (as specified in the next figure). Using the ping command, register and justify the pairs of equipment (including Switch 1) that have connectivity. Once again, verify that only equipment in the same VLAN has IP connectivity.



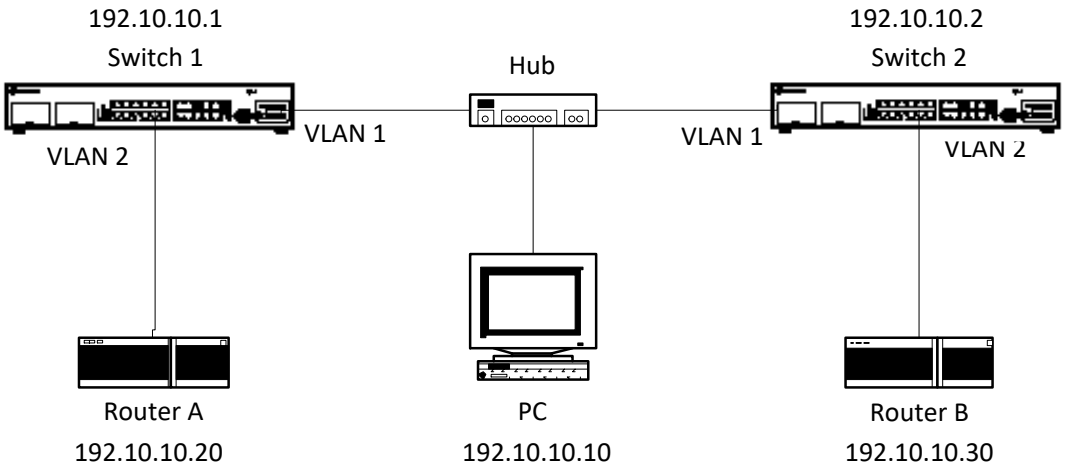
2.2. Using the RS-232 console access to the equipment, register and justify the MAC Address Table of Switch 1.

2.3. In the current network setup, start a capture with the WireShark on the PC and set an appropriate filter to display ARP and ICMP packets. Using the RS-232 console access to the equipment, run the ping commands specified in the following table. For each run, register the connectivity and the filtered packets. Justify the results obtained on each case.

Ping from:	Ping to:	Connectivity (yes or no)	Filtered packets
Router A	Switch 1		
Router A	Router B		
Router A	192.10.10.34		

Router B	Switch 1		
Router B	Router A		
Router B	192.10.10.34		
Switch 1	Router B		
Switch 1	192.10.10.34		

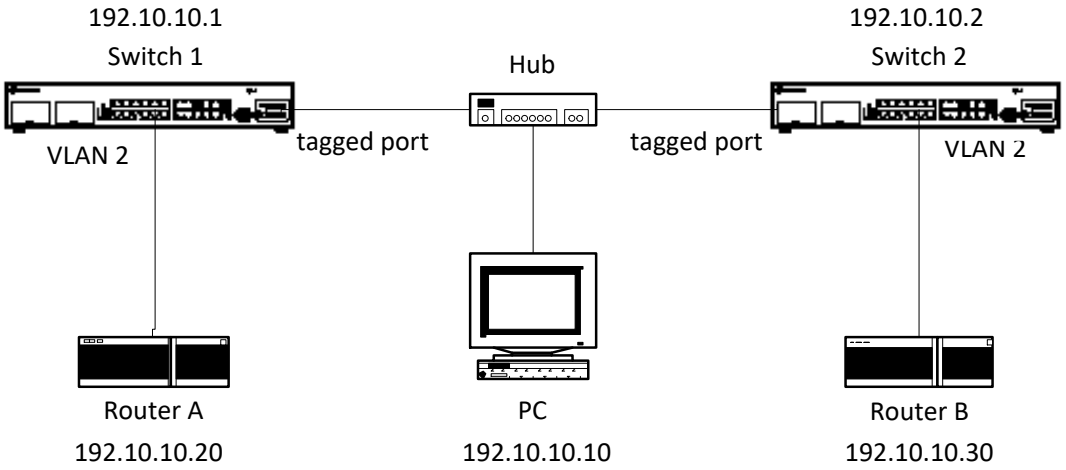
3. Reconfigure the network as specified in the following figure. In the new inserted Switch 2, configure VLANs 1 and 2 in the same way as specified to Switch 1 in the previous experiments. Note that in this case, only VLAN 1 is defined over the two switches.



3.1. In this network setup, start a capture with the WireShark on the PC and set an appropriate filter to display ARP and ICMP packets. Using the RS-232 console access to the equipment, run the ping commands specified in the following table. For each run, register the connectivity and the filtered packets. Justify the results obtained on each case.

Ping from:	**Ping to:**	**Connectivity (yes or no)**	**Filtered packets**
Router A	Switch 1		
Router A	Switch 2		
Router A	Router B		
Switch 1	Router A		
Switch 1	Switch 2		
Switch 1	Router B		

4. At both Switches 1 and 2, configure the port connected to the Hub as a tagged port in order to support both VLANs using the IEEE802.1Q VLAN protocol, as specified in the following figure.



4.1. In this network setup, start a capture with the WireShark on the PC and set an appropriate filter to display ARP and ICMP packets. Using the RS-232 console access to the equipment, run the ping commands specified in the following table. For each run, register the filtered packets and their VLAN ID value. Justify the results obtained on each case. For each case, compare these results with the ones observed in experiment 3.1.

Ping from:	Ping to:	VLAN ID	Filtered packets
Router A	Switch 1		
Router A	Switch 2		
Router A	Router B		
Switch 1	Router A		
Switch 1	Switch 2		
Switch 1	Router B		

☞ **Format of the Ethernet frames with and without 802.1Q tags**

Ethernet frame without 802.1Q tag

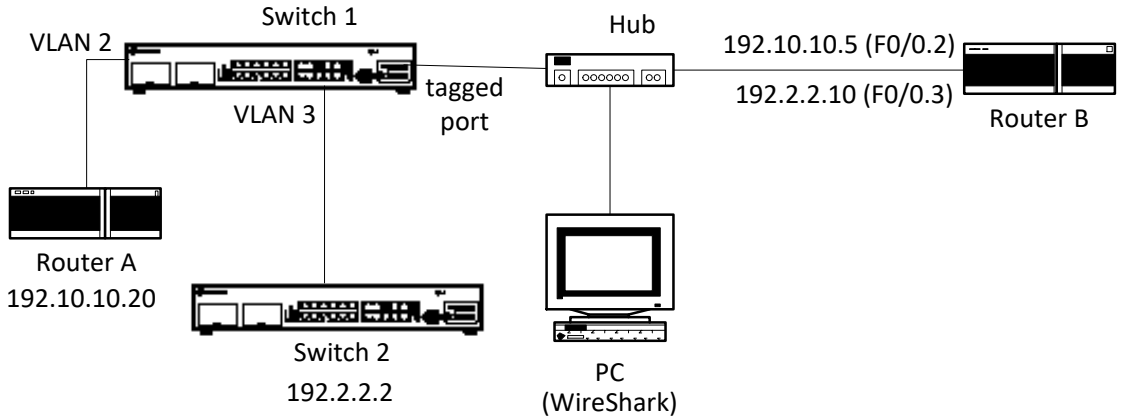
Destination Address (6 *bytes*)
Source Address (6 *bytes*)
Type / Length (2 *bytes*)
Data Field

Ethernet frame with 802.1Q tag

Destination Address (6 *bytes*)
Source Address (6 *bytes*)
8100h (2 *bytes*)
Priority (3 *bits*)
CFI (1 *bit*)
VLAN ID (12 *bits*)
Type / Length (2 *bytes*)
Data Field

5. Reconfigure the network as specified in the following figure where Router B routes packets between VLAN 2 and VLAN 3 (each one with its own network IP address).

- In Switch 1, configure the VLANs in the following way:
  a) ports numbered 1 to 4 belonging to VLAN 2;
  b) ports numbered 5 to 7 belonging to VLAN 3;
  c) port numbered 8 as a tagged port belonging to both VLAN 2 and 3.
- In Switch 2, set all ports in the default VLAN 1 and configure the given IP address.
- In Router B, create 2 virtual interfaces on interface F0/0, one for VLAN 2 (F0/0.2) and another for VLAN 3 (F0/0.3), with the given IP addresses.
- In both Switch 2 and Router A, configure the appropriate Default Gateway addresses.



☞ Configuration of virtual interfaces in Cisco *routers*

In order to configure 2 virtual interfaces on interface F0/0, one for VLAN 2 (F0/0.2) and another for VLAN 3 (F0/0.3), use the following commands:

`Router#configure terminal`	Enter global configuration mode
`Router(config)#interface f0/0`	Enter interface configuration mode
`Router(config-if)#no ip address`	Clean the IP address of the physical interface
`Router(config-if)#no shutdown`	Activate the interface
`Router(config-if)#interface f0/0.2`	Enter virtual interface configuration mode
`Router(config-subif)#encapsulation dot1Q 2`	Associate virtual interface to VLAN tag
`Router(config-subif)#ip address 192.10.10.5 255.255.255.0`	Configure IP address and subnet mask
`Router(config-if)#interface f0/0.3`	Enter virtual interface configuration mode
`Router(config-subif)#encapsulation dot1Q 3`	Associate virtual interface to VLAN tag
`Router(config-subif)#ip address 192.2.2.10 255.255.255.0`	Configure IP address and subnet mask
`Router(config-subif)#end`	Exit global configuration mode

☞ Configuration of Default Gateway in Cisco *routers*

In routers, a Default Gateway is a static route to another router for any network address that is not known by other means. Therefore, use the following commands in Router A:

`Router#configure terminal`	Enter global configuration mode
`Router(config)#ip route 0.0.0.0 0.0.0.0 192.10.10.5`	Define the next hop to any unknown network as 192.10.10.5
`Router(config)#end`	Exit global configuration mode

5.1. In order to verify the correctness of the configurations, check the IP connectivity between Switch 2 and Router A with the ping command. Register and justify the IP routing table of Router B.

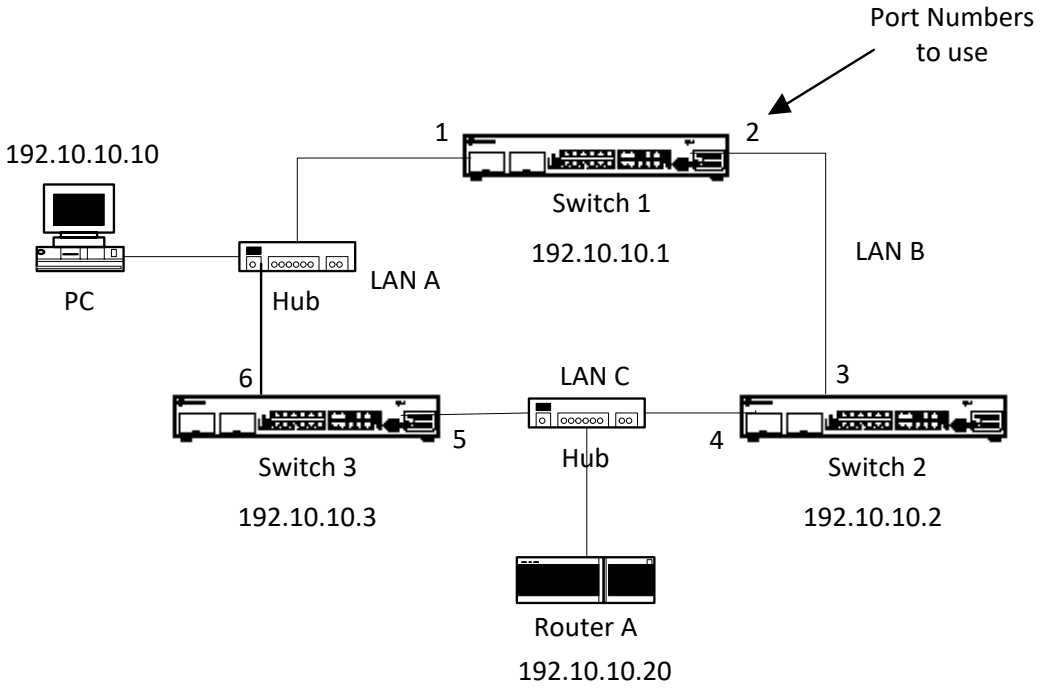
6. Using the RS-232 console access to the equipment, run the ping commands specified in the following table. For each run, register the filtered packets and their VLAN ID value. Justify the results obtained on each case.

Ping from:	**Ping to:**	**Filtered packets (and VLAN ID of each)**
Router A	Router B	
Router A	Switch 2	
Router A	192.2.2.27	
Switch 2	Router B	
Switch 2	Router A	
Switch 2	192.2.2.27	

5. Experiments with Spanning Tree Protocol

IMPORTANT NOTE:	Each switch has on its box an indication of its MAC address. In all next experiments, use the switch with lowest MAC address as Switch 1 and the switch with highest MAC address as switch 3.

7. Configure the network as specified in the figure below with the specified IP addresses (considering them as class C addresses). Note that the figure also specifies the port numbers that should be used on each switch. If necessary, eliminate previous created VLANs and disable the Spanning Tree protocol at all switches. At the PC, start a capture with WireShark and execute a *ping* command to an inexistent address of your IP network. Check that the ARP request messages sent by the PC are continuously circulating on your network generating a lot of traffic (many captured packets) and continuous network activity (signalled by the led lights of the switches). Why does this happen?



8. Disconnect one of the cables that are interconnecting the switches. Activate the Spanning Tree protocol in all switches using commands:

```
config stp version stp
enable stp
```

and connect again the disconnected cable. Wait for about 30 seconds to allow the spanning tree complete configuration. Verify, using the *ping* command, that you have connectivity between all five IP addresses. Register the MAC address table of the 3 switches. Based on the observed tables, determine the switch port that was blocked by the Spanning Tree protocol.

9. Remember how Spanning Tree protocol works: (i) the switch with the lowest *BridgeID* becomes the Root Bridge; (ii) the port on each switch (besides the Root Bridge) providing the lowest Root Path Cost to the Root Bridge becomes the Root Port of the switch and (iii) the port of each LAN providing the lowest Root Path Cost to the Root Bridge becomes the Designated Port of the LAN. Then, all switches activate their Root and Designated Ports and deactivate all other ports.

9.1. Using the commands:

```
show switch
show stp
show stp ports
```

determine the *BridgeID* of each switch and *PortCost* values of each active port on each switch. Register also the state (forwarding or discarding) of each active port on each switch and the root ports assumed by each switch.

9.2. Based on the *BridgeID* and *PortCost* values of the switches, determine the Root Bridge and the Root and Designated Ports on each switch (using your knowledge on how Spanning Tree protocols works). Confirm that they are in accordance with the observations of 9.1.

9.3. Confirm that the port states observed in 9.1 are in accordance with the Spanning Tree determined in 9.2 and the MAC address tables observed in 8.

10. Using Wireshark on your PC, capture and register the content of some BPDU packets. Disconnect your PC from LAN A and connect it to LAN C. Capture again and register the content of some BPDU packets. Based on the analysis of both captures, explain how Spanning Tree protocol maintains a spanning tree.

☞ **Format of configuration BPDU packets**

#octets				
2	Protocol Identifier			
1	Version			
1	Message Type			
1	TCA	Reserved		TC
8	Root ID			
4	Cost of Path to Root			
8	Bridge ID			
2	Port ID			
2	Message Age			
2	Max Age			
2	Hello Time			
2	Forward Delay			

11.1. Connect the PC back to LAN A. Analyse the current spanning tree checking the available routing path between the PC and Router A. Propose a solution (don't implement it, yet) to change this routing path based on changing only one *PortCost* value of one switch.

11.2. First, run a non-stop ping command from the PC to Router A. Then, implement the solution proposed in 11.1 and estimate the time duration of the temporarily lost of connectivity between the PC and Router A. Stop the ping command and justify the observed lost duration based on the different states of a port when changing from blocking to forwarding.

11.3. Register and analyse the state and the role of each active port on each switch and confirm the correctness of the solution implemented in 11.1.

12.1. Start a capture of BPDU packets. Consider the Designated Bridge of LAN C in the current network configuration. Change the *PortCost* value of one of its active ports in order to change the switch Root Port to the other active port. Since a change in the spanning tree parameters occurred, the topology change notification mechanism is triggered. Extend the capture for a period of at least 1 minute after the *PortCost* value change. Analyze the sequence of captured packets and verify if any TCN type BPDU packet was sent and if any change occurred in the TC and TCA flags of the configuration BPDUs.

☞ **Format of TCN (Topology Change Notification) BPDU packets**

#octets	
2	Protocol Identifier
1	Version
1	Message Type

12.2. Disconnect your PC from LAN A and connect it to LAN C. Cancel the previous change and wait for a period of about 1 minute in order for the original spanning tree to reconfigure itself. Then, repeat the previous change and analyze the sequence of captured packets on LAN C. Based on the analysis of 12.1 and 12.2., explain how the topology change notification mechanism of the Spanning Tree protocol works.

13. Connect the PC back to LAN A. For each of the three switches, execute the following sequence of actions:

(i) change the switch Spanning Tree *Hello Time* value to 6 seconds;

(ii) capture some BPDU packets and analyze their periodicity;

(iii) change the switch *Hello Time* value to its original value.

With these observations, you should verify that the *Hello Time* used by all switches is the one configured in the Root Bridge, whatever value is configured in the other switches.